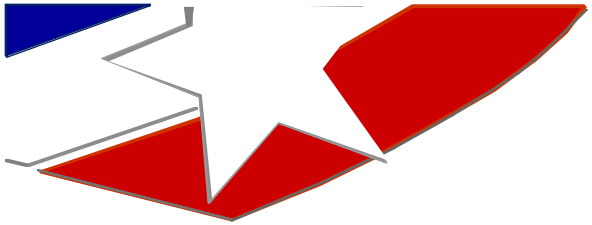


Certificates in Public Key Infrastructures

John Long

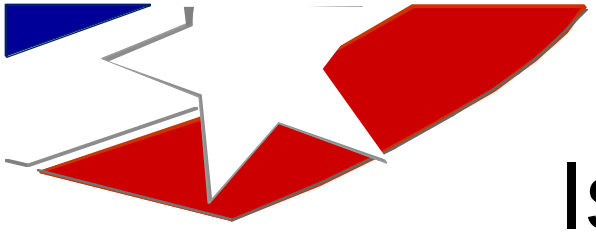
Jplong@sandia.gov

Sandia is a multiprogram laboratory operated by Sandia Corporation,
a Lockheed Martin Company, for the United States Department of Energy
under Contract DE-AC04-94AL85000.

Information released under SAND No. 98-1098C.

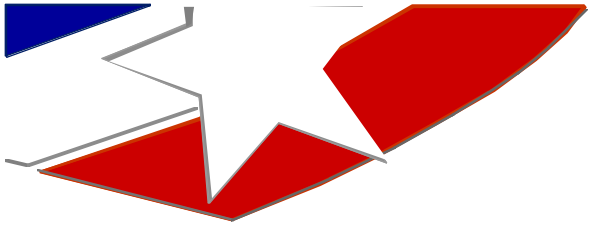
Computer Security
Technologies

Sandia National Laboratories



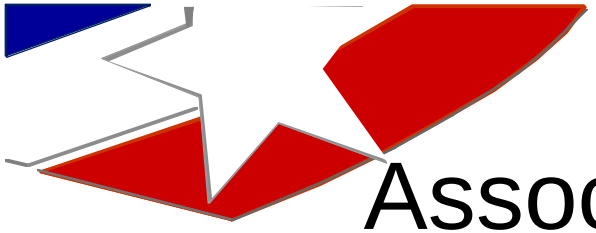
Issuing Certificates

- Identify applicant
- Associate applicant with key
- Provide applicant with CA public key



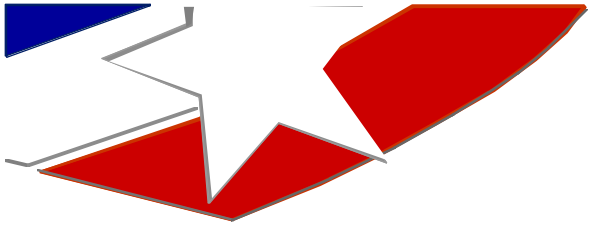
Identify Applicant

- Rigor of identification depends on certificate usage
- Furnish e-mail address
- Driver's license, credit card
- Present DOE badge in person



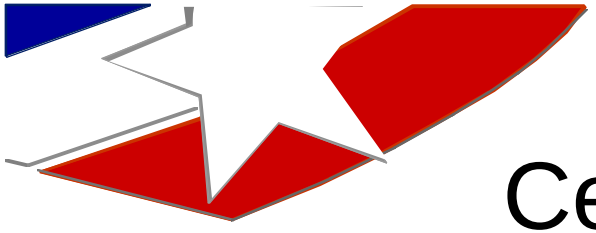
Associate applicant with key

- Establish secure session with applicant
- Generate keys under supervision by server
  - or
- Client presents keys using web browser
- Is the key unique?



Provide applicant with CA public key

- Download during secure session
- Trust any CA claiming the right name

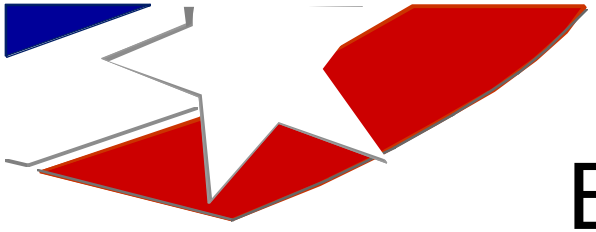


Certificate distribution

- “Good Buddy” system
- Repository
- Directory supervised by CA, chained

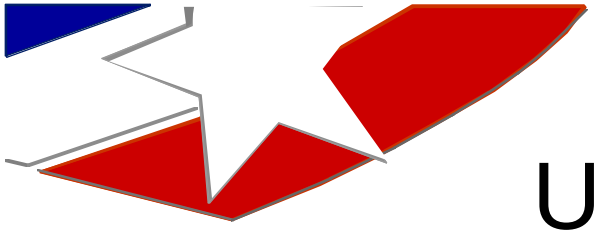
Computer Security
Technologies

Sandia National Laboratories



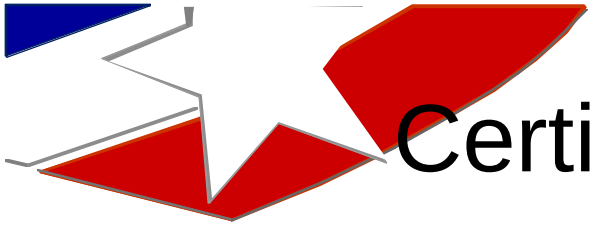
Backup / Archiving

- CA builds key histories for clients
- CA is backed up regularly
- CA backs up dated copy of key archive



Unique identification

- Several people with same or similar names
- Pointers to other databases
- Tied to organizational information

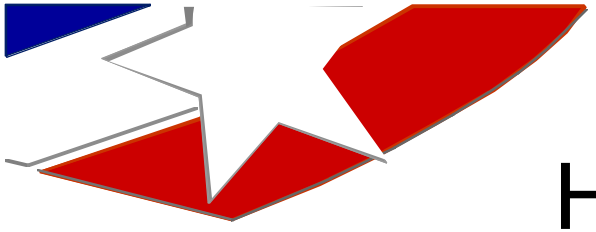


Certificate Policy / Practice Statement

- Sets forth legal limitations on certificate use
- Outlines CA operational security
- Provides CA procedure guidelines
- Practice statement provides details on CA operation

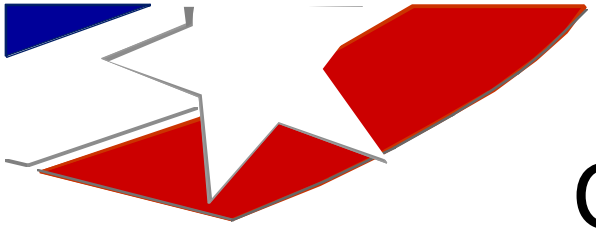
Computer Security Technologies

Sandia National Laboratories



Hierarchies of CA's

- Touted advantages not there
- Contradiction in supposed capabilities

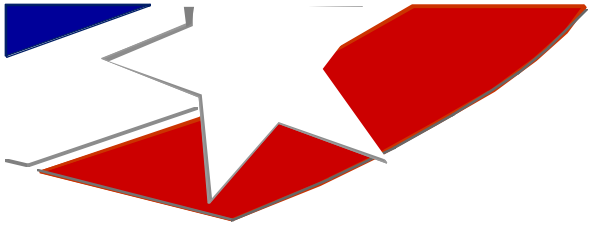


Cross Certification

- Be sure security of CA is understood
- Trust level of certificate is determined
- Provides secure copy of CA certificate to other CA
- Chains directories to provide auto certificate retrieval

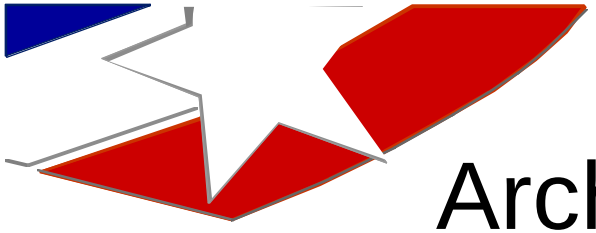
Computer Security
Technologies

Sandia National Laboratories



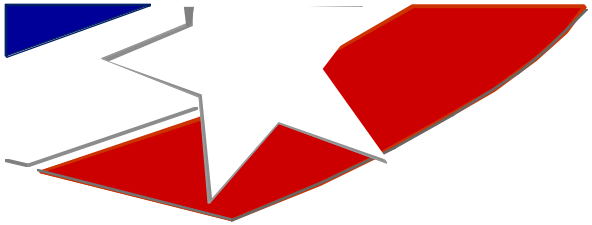
Security issues

- CA's may become lax
- Compromise of a CA
- Compromise of a client



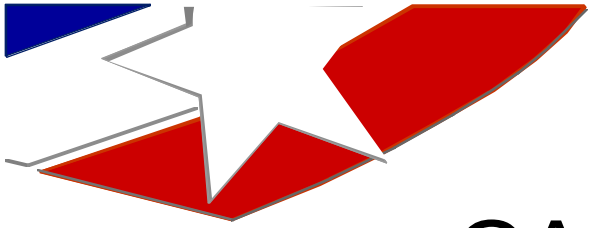
Archiving encrypted data

- Disk in a desk
- Archive and forget it



CA services

- Identification / issue certificate
- Protection when password is forgotten
- Protection when key is updated
- Identification of other CA's
- Automatic retrieval of certificates
- Limiting legal liability
- Documentation for legal challenges



CA services (continued)

- Recovery of files if employee absent
- Meeting requirements for contracts, disbursing funds